

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-69137

(43) 公開日 平成11年(1999) 3月9日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 N 1/387

H 0 4 N 1/387

G 0 9 C 1/00

G 0 9 C 1/00

6 3 0 A

6 3 0

6 6 0 D

6 6 0

5/00

5/00

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

審査請求 未請求 請求項の数15 O L (全 14 頁) 最終頁に続く

(21) 出願番号

特願平9-223930

(22) 出願日

平成9年(1997) 8月20日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

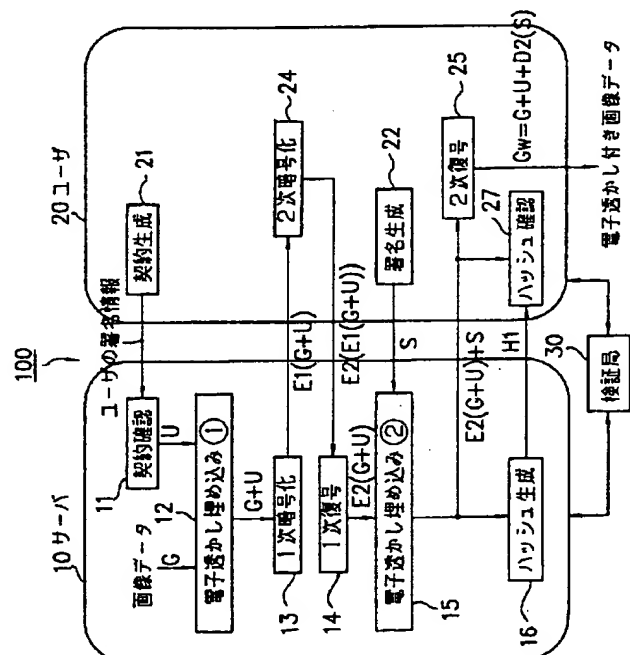
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 電子透かし方式、電子情報配布システムおよび画像ファイル装置

(57) 【要約】

【課題】 著作権に係るデジタルデータの不正コピーを確実に防止できる電子透かし方式を提供する。

【解決手段】 複数のエンティティ間で送受信されるデジタル情報（画像データG）に対して電子透かし情報の埋め込み処理を行うエンティティ（サーバ端末装置10）と、暗号処理を行うエンティティ（ユーザ端末装置20）とを別に設けることにより、サーバまたはユーザがデジタルデータを不正にコピーして配布を行った際にその不正行為を確実に認識することができるようにする。また、このシステムでは、サーバとユーザの利害は相反するので、両者が結託して不正することはあり得ず、デジタルデータの不正配布に関して安全なシステムを実現できる。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項 1】 電子透かし情報の埋め込まれたデータに対して少なくとも暗号化および復号の一方の処理を行うことを特徴とする電子透かし方式。

【請求項 2】 電子透かし情報が埋め込まれ、且つ、暗号化されたデータに対して、別の情報を更に電子透かし情報として埋め込むことを特徴とする電子透かし方式。

【請求項 3】 上記別の情報を更に電子透かし情報として埋め込むデータは、上記電子透かし情報が埋め込まれた状態で暗号化されていることを特徴とする請求項 2 に記載の電子透かし方式。

【請求項 4】 上記暗号化とは異なる暗号化を施した後上記別の情報を更に電子透かし情報として埋め込むことを特徴とする請求項 2 または 3 に記載の電子透かし方式。

【請求項 5】 共通のデータに対して暗号化を行う前と、当該暗号化を行う後に、互いに異なる情報をそれぞれ電子透かし情報として埋め込むことを特徴とする電子透かし方式。

【請求項 6】 複数のエンティティを含むネットワークシステムで用いられる電子透かし方式であって、上記複数のエンティティ間で送受信される暗号化されたデータに対して電子透かしを埋め込むエンティティと、上記暗号処理およびそれに対応する復号処理を実行するエンティティとを別に有することを特徴とする電子透かし方式。

【請求項 7】 上記データが画像データであることを特徴とする請求項 1 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 8】 複数のエンティティからなるネットワークシステム上でデジタル情報の送受信を行う電子情報配布システムにおいて、上記デジタル情報に対して電子透かし情報の埋め込み処理を行う第 1 のエンティティと、上記デジタル情報に対して暗号処理およびそれに対応する復号処理を行う第 2 のエンティティとを有することを特徴とする電子情報配布システム。

【請求項 9】 複数のエンティティからなるネットワークシステムにおいて、第 1 のエンティティと第 2 のエンティティとがデジタル情報の送受信を行う場合、上記第 1 のエンティティは、上記第 2 のエンティティにより暗号化された情報を受け取り、電子透かし情報の埋め込み処理を行って上記第 2 のエンティティに送信し、上記第 2 のエンティティは、上記第 1 のエンティティより受け取った情報に上記暗号化に対する復号処理を行うことを特徴とする電子情報配布システム。

【請求項 10】 複数のエンティティからなるネットワークシステムにおいて、第 1 のエンティティと第 2 のエンティティとがデジタル情報の送受信を行う場合、上記第 1 のエンティティは、第 1 の暗号化の前に電子透

かし情報の埋め込み処理を行って、得られた情報を上記第 2 のエンティティに送信し、

上記第 2 のエンティティは、上記第 1 のエンティティより受け取った情報に第 2 の暗号化を行って、得られた情報を上記第 1 のエンティティに送信し、

上記第 1 のエンティティは、上記第 2 のエンティティより受け取った情報に対して上記第 1 の暗号化に対する第 1 の復号処理を行った後に電子透かし情報の埋め込み処理を行って、得られた情報を上記第 2 のエンティティに送信し、

上記第 2 のエンティティは、上記第 1 のエンティティより受け取った情報に対して上記第 2 の暗号化に対する第 2 の復号処理を行うことを特徴とする電子情報配布システム。

【請求項 11】 上記第 1 のエンティティが埋め込む電子透かし情報は、上記第 2 のエンティティに関する情報を含むことを特徴とする請求項 8 ～ 10 の何れか 1 項に記載の電子情報配布システム。

【請求項 12】 上記第 1 のエンティティが埋め込む電子透かし情報は、送信するデジタル情報に関する情報を含むことを特徴とする請求項 8 ～ 11 の何れか 1 項に記載の電子情報配布システム。

【請求項 13】 上記第 1 のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第 2 のエンティティの署名を検証することを特徴とする請求項 8 ～ 12 の何れか 1 項に記載の電子情報配布システム。

【請求項 14】 暗号化されていた画像情報を復号して得た画像情報と、暗号化された状態で付加され上記画像情報と共に復号処理の施された電子透かし情報とを画像データとして格納することを特徴とする画像ファイル装置。

【請求項 15】 上記画像データとは別途、上記暗号化に係わる鍵情報を格納することを特徴とする請求項 14 に記載の画像ファイル装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は電子透かし方式、電子情報配布システムおよび画像ファイル装置に関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のデジタル情報における著作権を保護するための電子透かし技術、それを用いてデジタル情報の配布を行うマルチメディアネットワークおよびそれを用いた画像ファイル装置に用いて好適なものである。

【0002】

【従来の技術】 近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品として、例えば画像

10

20

30

40

50

3

等を含むデジタルデータが考えられる。しかし、デジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのデジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配布できるという可能性を示す。これにより、本来デジタルデータの著作権または著作権から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【0003】一方、著作権または販売者（以下、これらのデジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにデジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。そのため、不正コピーを直接防止するのではなく、電子透かしと呼ばれる手法が提案されている。この電子透かしとは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する著作権情報やユーザに関する利用者情報をデジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【0004】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく不正を行う可能性があるとする、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【0005】これは、図10に示すように、従来のシステムでは、ユーザを特定するための利用者情報d1をデジタルデータ（以下、デジタルデータを画像データとして説明する）gにサーバが埋め込むので、サーバが勝手に利用者情報d1を埋め込んでそのコピーを不正に配布した場合、その利用者情報d1から特定されるユーザ（図10の例ではユーザU）は、サーバの主張を退ける手段がないためである。

【0006】その対策として、例えば、「B.Pfitmann and M.Waidner: "Asymmetric Fingerprinting," EUROCRYPT'96」の文献（以下、文献1と言う）に、公開鍵暗号方式を用いたシステム（図11）が提案されている。ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、RSA暗号やElGamal暗号等が知られている。以下、公開鍵暗号方式における（a）特徴、（b）秘密通信や認証通信等のプロトコルについて述べる。

【0007】（a）公開鍵暗号の特徴

（1）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（2）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

4

（3）送られてきた通信文の送信者が偽者でないこと、およびその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0008】（b）公開鍵暗号のプロトコル

例えば、通信文Mに対して、公開の暗号鍵 k_p を用いて行う暗号化操作を $E(k_p, M)$ とし、秘密の復号鍵 k_s を用いて行う復号操作を $D(k_s, M)$ とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

10 （1）暗号鍵 k_p が与えられたとき、暗号化操作 $E(k_p, M)$ の計算は容易である。また、復号鍵 k_s が与えられたとき、復号操作 $D(k_s, M)$ の計算は容易である。

（2）もしユーザが復号鍵 k_s を知らないなら、暗号鍵 k_p と、暗号化操作 $E(k_p, M)$ の計算手順と、暗号文 $C = E(k_p, M)$ とを知っていても、通信文Mを決定することは計算量の点で困難である。

20 【0009】次に、上記（1）、（2）の条件に加えて、次の（3）の条件が成立することにより秘密通信機能を実現できる。

（3）全ての通信文（平文）Mに対し暗号化操作 $E(k_p, M)$ が定義でき、

$$D(k_s, E(k_p, M)) = M$$

が成立する。つまり、暗号鍵 k_p は公開されているため、誰もが暗号化操作 $E(k_p, M)$ の計算を行うことができるが、 $D(k_s, E(k_p, M))$ の計算をして通信文Mを得ることができるのは、秘密の復号鍵 k_s を持っている本人だけである。

30 【0010】一方、上記（1）、（2）の条件に加えて、次の（4）の条件が成立することにより認証通信機能を実現できる。

（4）全ての通信文（平文）Mに対し復号操作 $D(k_s, M)$ が定義でき、

$$E(k_p, D(k_s, M)) = M$$

が成立する。つまり、復号操作 $D(k_s, M)$ の計算ができるのは秘密の復号鍵 k_s を持っている本人のみであり、他の人が偽の秘密の復号鍵 k_s' を用いて $D(k_s', M)$ の計算を行い、秘密の復号鍵 k_s を持っている本人になりすましたとしても、

$$40 \quad E(k_p, D(k_s', M)) \neq M$$

であるため、受信者は受けとった情報が不正なものであることを確認できる。また、 $D(k_s, M)$ の値が改ざんされても、

$$E(k_p, D(k_s, M)') \neq M$$

となり、受信者は受けとった情報が不正なものであることを確認できる。

【0011】上述のような公開鍵暗号方式では、公開の暗号鍵（以下、公開鍵とも言う） k_p を用いる処理 $E()$ を「暗号化」、秘密の復号鍵（以下、秘密鍵とも言う） k_s を用いる処理 $D()$ を「復号」と呼んでいる。したが

5

って、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【0012】以下に、公開鍵暗号方式により送信者Aから受信者Bへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者Aの秘密鍵を $k_s A$ 、公開鍵を $k_p A$ とし、受信者Bの秘密鍵を $k_s B$ 、公開鍵を $k_p B$ とする。

【0013】[秘密通信]送信者Aから受信者Bへ通信文(平文)Mを秘密通信する場合は、次の手順で行う。

Step1: 送信者Aは、受信者Bの公開鍵 $k_p B$ で通信文Mを以下のように暗号化し、暗号文Cを受信者Bに送る。

$$C = E(k_p B, M)$$

Step2: 受信者Bは、自分の秘密鍵 $k_s B$ で暗号文Cを以下のように復号し、もとの平文Mを得る。

$$M = D(k_s B, C)$$

なお、受信者Bの公開鍵 $k_p B$ は不特定多数に公開されているので、送信者Aに限らず全ての人が受信者Bに秘密通信できる。

【0014】[認証通信]送信者Aから受信者Bへ通信文(平文)Mを認証通信する場合は、次の手順で行う。

Step1: 送信者Aは、自分の秘密鍵 $k_s A$ で送信文Sを以下のように生成し、受信者Bに送る。

$$S = D(k_s A, M)$$

この送信文Sを「署名文」と言い、署名文Sを得る操作を「署名」と言う。

Step2: 受信者Bは、送信者Aの公開鍵 $k_p A$ で署名文Sを以下のように復元変換し、もとの平文Mを得る。

$$M = E(k_p A, S)$$

もし、通信文Mが意味のある文であることを確認したならば、通信文Mが確かに送信者Aから送られてきたことを認証する。送信者Aの公開鍵 $k_p A$ は不特定多数に公開されているので、受信者Bに限らず全ての人が送信者Aの署名文Sを認証できる。このような認証を「デジタル署名」とも言う。

【0015】[署名付秘密通信]送信者Aから受信者Bへ通信文(平文)Mを署名付秘密通信する場合は、次の手順で行う。

Step1: 送信者Aは、自分の秘密鍵 $k_s A$ で通信文Mを以下のように署名し、署名文Sを作る。

$$S = D(k_s A, M)$$

さらに、送信者Aは、受信者Bの公開鍵 $k_p B$ で署名文Sを以下のように暗号化し、暗号文Cを受信者Bに送る。

$$C = E(k_p B, S)$$

Step2: 受信者Bは、自分の秘密鍵 $k_s B$ で暗号文Cを以下のように復号し、署名文Sを得る。

$$S = D(k_s B, C)$$

さらに、受信者Bは、送信者Aの公開鍵 $k_p A$ で署名文

6

Sを以下のように復元変換し、もとの平文Mを得る。

$$M = E(k_p A, S)$$

もし、通信文Mが意味のある文であることを確認したならば、通信文Mが確かに送信者Aから送られてきたことを認証する。

【0016】なお、署名付秘密通信の各Step内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、

$$\text{Step1: } C = E(k_p B, D(k_s A, M))$$

$$10 \quad \text{Step2: } M = E(k_p A, D(k_s B, C))$$

となっているが、下記のような手順でも署名付秘密通信が実現できる。

$$\text{Step1: } C = D(k_s A, E(k_p B, M))$$

$$\text{Step2: } M = D(k_s B, E(k_p A, C))$$

【0017】以下に、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム(上記図1)における操作の手順を示す。

1) まず、サーバとユーザ間で画像データgの売買に関する契約書d2を取り交わす。

20 【0018】2) 次に、ユーザは、自分を示す乱数IDを発生させ、これを用いて一方向性関数fを生成する。この一方向性関数とは、関数 $y = f(x)$ において、xからyを求めることは容易だが、逆にyからxを求めることが困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散的対数等が一方向性関数としてよく用いられる。

3) 次に、ユーザは、契約書d2と一方向性関数fに対して、自分の秘密鍵 $k_s U$ を用いて署名情報d3を生成し、それらを合わせてサーバに送る。

30 【0019】4) 次に、サーバは、ユーザの公開鍵 $k_p U$ を用いて署名情報d3と契約書d2を確認する。

5) サーバは確認後、現在までの全配布記録d4と、ユーザが作成した乱数IDとを画像データgに埋め込み、電子透かし付き画像データ($g + d4 + ID$)を生成する。

6) サーバは、ユーザにその電子透かし付き画像データ($g + d4 + ID$)を送る。

【0020】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに含まれるIDからユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定するIDはユーザ自身によって生成され、それを用いた一方向性関数値fにユーザの署名が付けられるので、サーバは任意のユーザに対してそのようなIDを生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定するIDをサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。

【0021】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム（図12）が、「三浦、渡辺、嵩（奈良先端大）：“サーバの不正も考慮した電子透かしについて”，SCIS97-31C」の文献（以下、文献2と言う）に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時および復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図12のシステムにおける操作の手順を示す。

【0022】1）まず、ユーザが原画像サーバに所望の画像データを、署名 d_5 を付けて要求する。

2）原画像サーバは、その要求内容をユーザの署名 d_5 から確認し、その確認後に、要求された画像データ g を暗号化して埋め込みサーバに送る。このとき、原画像サーバは、ユーザ名 u および委託内容 d_6 に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数 f' をユーザに送る。

【0023】3）埋め込みサーバは、送られてきた暗号化画像データ g' と、署名 $(u + d_6)$ とを確認し、ユーザ名 u および委託内容 d_6 を基にユーザを特定する利用者情報 d_7 の作成および埋め込みを行い、電子透かし付き暗号化画像データ $(g' + d_7)$ を作成する。その後、埋め込みサーバは、その電子透かし付き暗号化画像データ $(g' + d_7)$ をユーザに送る。

4）ユーザは、原画像サーバから送られてきた復号関数 f' を用いて、電子透かし付き暗号化画像データ $(g' + d_7)$ を電子透かし付き画像データ $(g + d_7)$ へと復号する。

【0024】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報 d_7 を画像データ g に埋め込んでおらず、また、埋め込みサーバは復号関数 f' を知らない（画像を元に戻せない）ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報 d_7 を無断で埋め込んだ画像データを不正配布できないことを根拠にしている。

【0025】しかしながら、この図12のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、埋め込みサーバが原画像である画像データ g の暗号化画像データ g' を持ち、ユーザが復号関数 f' を持つため、原画像サーバと埋め込みサーバとが結託した場合には、上述の図11のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には、原画像の不正入手が可能である。

【0026】また、原画像サーバは復号関数 f' をユー

ザに送るが、ユーザの復号関数 f' の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数 f' を知ることができる可能性は大きい。

【0027】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、または正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。これは、埋め込みサーバは自分の署名などを埋め込まないので、埋め込み情報と利用者情報の対応のみが埋め込みサーバの秘密であるが、データベース等を用いた埋め込み情報と利用者情報のランダムな対応ではなく、ある規則に基づいて利用者情報から埋め込み情報が作成される場合、解析される危険性は大きいからである。そして、この場合、上述の図11のシステムと同様の不正が可能である。

【0028】

【発明が解決しようとする課題】本発明はこのような実情に鑑みて成されたものであり、上述のようなサーバおよびユーザの不正を確実に防止できる電子透かし方式および電子情報配布システムを提供することを目的とする。

【0029】

【課題を解決するための手段】本発明の電子透かし方式は、電子透かし情報の埋め込まれたデータに対して少なくとも暗号化および復号の一方の処理を行うことを特徴とする。

【0030】本発明の他の特徴とするところは、電子透かし情報が埋め込まれ、且つ、暗号化されたデータに対して、別の情報を更に電子透かし情報として埋め込むことを特徴とする。ここで、上記別の情報を更に電子透かし情報として埋め込むデータは、上記電子透かし情報が埋め込まれた状態で暗号化されているものであっても良い。また、上記暗号化とは異なる暗号化を施した後上記別の情報を更に電子透かし情報として埋め込むようにしても良い。

【0031】本発明のその他の特徴とするところは、共通のデータに対して暗号化を行う前と、当該暗号化を行う後に、互いに異なる情報をそれぞれ電子透かし情報として埋め込むことを特徴とする。

【0032】本発明のその他の特徴とするところは、複数のエンティティを含むネットワークシステムで用いられる電子透かし方式であって、上記複数のエンティティ間で送受信される暗号化されたデータに対して電子透かしを埋め込むエンティティと、上記暗号処理およびそれに対応する復号処理を実行するエンティティとを別に対応することを特徴とする。以上の構成において、上記データは画像データであっても良い。

【0033】また、本発明の電子情報配布システムは、

10

20

30

40

50

複数のエンティティからなるネットワークシステム上でデジタル情報の送受信を行う電子情報配布システムにおいて、上記デジタル情報に対して電子透かし情報の埋め込み処理を行う第1のエンティティと、上記デジタル情報に対して暗号処理およびそれに対応する復号処理を行う第2のエンティティとを有することを特徴とする。

【0034】本発明の他の特徴とするところは、複数のエンティティからなるネットワークシステムにおいて、第1のエンティティと第2のエンティティとがデジタル情報の送受信を行う場合、上記第1のエンティティは、上記第2のエンティティにより暗号化された情報を受け取り、電子透かし情報の埋め込み処理を行って上記第2のエンティティに送信し、上記第2のエンティティは、上記第1のエンティティより受け取った情報に上記暗号化に対する復号処理を行うことを特徴とする。

【0035】本発明のその他の特徴とするところは、複数のエンティティからなるネットワークシステムにおいて、第1のエンティティと第2のエンティティとがデジタル情報の送受信を行う場合、上記第1のエンティティは、第1の暗号化の前に電子透かし情報の埋め込み処理を行って、得られた情報を上記第2のエンティティに送信し、上記第2のエンティティは、上記第1のエンティティより受け取った情報に第2の暗号化を行って、得られた情報を上記第1のエンティティに送信し、上記第1のエンティティは、上記第2のエンティティより受け取った情報に対して上記第1の暗号化に対する第1の復号処理を行った後に電子透かし情報の埋め込み処理を行って、得られた情報を上記第2のエンティティに送信し、上記第2のエンティティは、上記第1のエンティティより受け取った情報に対して上記第2の暗号化に対する第2の復号処理を行うことを特徴とする。

【0036】ここで、上記第1のエンティティが埋め込む電子透かし情報は、少なくとも上記第2のエンティティに関する情報および送信するデジタル情報に関する情報の一方を含むものであっても良い。

【0037】また、ここで、好適には上記第1のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第2のエンティティの署名を検証するようにする。

【0038】また、本発明の画像ファイル装置は、暗号化されていた画像情報を復号して得た画像情報と、暗号化された状態で付加され上記画像情報と共に復号処理の施された電子透かし情報とを画像データとして格納することを特徴とする。ここで、上記画像データとは別途、上記暗号化に係わる鍵情報を格納するようにしても良い。

【0039】

【発明の実施の形態】

〔第1の実施形態〕以下、本発明に係る第1の実施形態

を、図1を参照して説明する。本発明に係る電子透かし方式は、例えば、図1に示すようなシステム100により実施され、このシステム100は、本発明に係る電子情報配布システムを適用したものである。

【0040】すなわち、システム100は、サーバ側の端末装置（サーバ端末装置）10、ユーザ側の端末装置（ユーザ端末装置）20および検証局側の端末装置（検証局端末装置）30を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにデジタルデータの授受を行うようになされている。

【0041】サーバ端末装置10は、ユーザ端末装置20からのデータが供給される契約確認処理部11と、例えば画像データ（デジタルデータ）が供給される第1の電子透かし埋め込み処理部12と、上記第1の電子透かし埋め込み処理部12の出力が供給される1次暗号化処理部13と、ユーザ端末装置20からのデータが供給される1次復号処理部14と、ユーザ端末装置20からのデータおよび1次復号処理部14の出力が供給される第2の電子透かし埋め込み処理部15と、上記第2の電子透かし埋め込み処理部15の出力が供給されるハッシュ生成処理部16とを備えており、1次暗号化処理部13およびハッシュ生成処理部16の各出力がユーザ端末装置20に送信されるようになされている。また、第2の電子透かし埋め込み処理部15の出力は、ハッシュ生成処理部16に供給されるとともに、ユーザ端末装置20にも送信されるようになされている。

【0042】また、ユーザ端末装置20は、サーバ端末装置10の契約確認処理部11に対してデータ送信する契約生成処理部21と、署名生成処理部22と、サーバ端末装置10の1次暗号化処理部13からのデータが供給される2次暗号化処理部24と、サーバ端末装置10の第2の電子透かし埋め込み処理部15からのデータが供給される2次復号処理部25と、サーバ端末装置10の1次復号処理部14からのデータが供給される2次復号処理部25と、サーバ端末装置10の第2の電子透かし埋め込み処理部15およびハッシュ生成処理部16からのデータが供給されるハッシュ確認処理部27とを備えており、2次復号処理部25の出力が電子透かし付き画像データとして出力されるようになされている。また、2次暗号化処理部24の出力は、サーバ端末装置10の1次復号処理部14に供給され、署名生成処理部23の出力は、サーバ端末装置10の第2の電子透かし埋め込み処理部15に供給されるようになされている。

【0043】上述のようなシステム100では、方式や秘密鍵等の1次暗号に関する情報はサーバだけが知る情報であり、2次暗号に関する情報はユーザだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「E

i ()」、復号を「D i ()」で表わし、電子透かしに関する埋め込み処理を「+」で表わすものとする。

【0044】以下に、上記のように構成したシステム100の動作を説明する。まず、電子透かしに関する埋め込み処理について説明する。

【0045】[埋め込み処理]

1) まず、ユーザ端末装置20において、ユーザが署名を付けてサーバ端末装置10に所望の画像データを要求する。この要求データは、契約生成処理部21により生成された情報(ユーザの署名情報)であり、以下ではこれを契約情報と呼ぶ。

【0046】2) 次に、サーバ端末装置10において、契約確認処理部11は、受信した契約情報をユーザの署名から確認し、その確認後に、契約情報から利用者情報Uを作成する。そして、第1の電子透かし埋め込み処理部12は、上記契約確認処理部11で作成された利用者情報Uを要求された画像データGに埋め込む。また、1次暗号化処理部13は、第1の電子透かし埋め込み処理部12で利用者情報Uが埋め込まれた画像データ(G+U)に対して1次暗号化処理E1()を行い、得られたデータをユーザ端末装置20に送る。よって、ユーザ端末装置20には、1次暗号化画像データE1(G+U)の情報が送られることになる。

【0047】3) 次に、ユーザ端末装置20において、2次暗号化処理部24は、サーバ端末装置10から送られてきた1次暗号化画像データE1(G+U)に対して2次暗号化を行い、得られた2次暗号化画像データE2(E1(G+U))をサーバ端末装置10に送る。このとき、ユーザは、署名生成処理部22により自分の秘密鍵を用いて署名情報Sを生成し、サーバ端末装置10に送る。

【0048】4) 次に、サーバ端末装置10において、1次復号処理部14は、ユーザ端末装置20から送られてきた2次暗号化画像データE2(E1(G+U))の1次暗号化を復号する。また、第2の電子透かし埋め込み処理部15は、同じくユーザ端末装置20から送られてきた署名情報Sを確認し、確認した署名情報Sを、上記1次復号処理部14で生成されたE2(G+U)の情報に埋め込み、ユーザ端末装置20に送る。また、ハッシュ生成処理部16は、ユーザ端末装置20への送信データE2(G+U)+Sに対するハッシュ値H1を生成および署名し、上記送信データE2(G+U)+Sと共にユーザ端末装置20に送る。よって、ユーザ端末装置20には、E2(G+U)+Sの情報とハッシュ値H1、およびその署名が送られることになる。

【0049】なお、ハッシュ値とは、一般にハッシュ関数h()の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値x1、x2に対してh(x1)=h(x2)となることである。また、圧縮関数とは、任意のビット長のビット列

をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数h()で、h(x1)=h(x2)を満たす値x1、x2を容易に見出せないものである。このとき、任意の値yからy=h(x)を満たす値xを容易に見出せないため、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、MD(Message Digest)5やSHA(Secure Hash Algorithm)等が知られている。

【0050】5) 次に、ユーザ端末装置20において、ハッシュ確認処理部27は、サーバ端末装置10から送られてきたハッシュH1とその署名とを確認し、上記ハッシュ値H1と、E2(G+U)+Sの情報から生成されるハッシュ値とが一致することを確認する。そして、その確認後に上記E2(G+U)+Sの情報およびハッシュ値H1とその署名を保存する。さらに、2次復号処理部25は、サーバ端末装置10から送られてきたE2(G+U)+Sの情報の2次暗号化を復号して電子透かし付き画像データGwを取り出す。よって、電子透かし付き画像データGwは、 $Gw = G + U + D2(S)$ と表わされる。これは、元の画像データGに利用者情報Uと2次暗号の影響を受けた署名情報Sとが透かし情報として埋め込まれていることを示す。

【0051】以上のように、本実施形態による電子透かし方式によれば、電子透かし情報の埋め込みは全てサーバ側で行うので、ユーザは基本的に不正をすることができない。サーバ側では、ユーザ側から署名情報Sを直接受け取ってそれを電子透かし情報として埋め込むが、上記埋め込み処理中の5)の変換手順によってユーザ端末装置20で得られた署名情報D2(S)は、ユーザのみが知る2次暗号化の影響を受けたものであるため、サーバは署名情報D2(S)を直接原画像に埋め込んでユーザに罪を着せることはできない。

【0052】そこで、不正コピー(不正画像)が発見された場合は、以下のような検証処理によって不正者の特定を行う。ただし、ここでは上述の文献1、文献2と同様に、画像データは透かし情報の変形および消去を受けないものとする。

【0053】[検証処理]

1) まず、サーバ端末装置10において、発見した不正画像 $Gw' = G + U' + D2(S')$ から利用者情報U'を抽出する。

2) サーバ端末装置10は、不正画像Gw'と抽出した利用者情報U'とを検証局30に示し、ユーザへの検査を要求する。

3) 検証局30は、ユーザが保存している2次暗号の鍵の提出を求め、提出された暗号鍵を使って不正画像Gw'を2次暗号化することにより、署名情報S'の抽出を行う。

【0054】4) ここで、正しい署名情報が抽出された

場合 ($S' = S$ の場合) には、ユーザの不正と認定する。

5) また、正しい署名情報が抽出されなかった場合

($S' \neq S$ の場合) には、検証局 30 は、さらにサーバ端末装置 10 からユーザ端末装置 20 に送られてきた $E2 (G+U) + S$ の情報とそのハッシュ値 $H1$ とその署名との提出をユーザに求め、ハッシュ値 $H1$ とその署名とを確認し、上記ハッシュ値 $H1$ と、 $E2 (G+U) + S$ の情報から生成されるハッシュ値とが一致することを確認する。そして、その確認後に、検証処理の 3) の手順でユーザから提出された 2 次暗号の鍵を用いて上記 $E2 (G+U) + S$ の情報を復号して、電子透かし付き画像データ Gw を取り出す。

【0055】6) ここで、正しい電子透かし付き画像データが取り出せなかった場合は、ユーザの不正と認定する。これは、上記検証処理中の 3) の手順で提出された 2 次暗号の鍵が正しくないことを意味する。

7) 一方、正しい電子透かし付き画像データが取り出せた場合は、サーバの不正と認定する。

以上の検証処理の手順から明らかなように、検証局 30 の端末装置は、ユーザ端末装置 20 内の 2 次暗号化処理部 24、2 次復号処理部 25、ハッシュ確認処理部 27 と同様の処理機能を有している。

【0056】以上のことにより、本実施形態によれば、サーバとユーザの利害は相反するので両者の結託はありえない。これにより、ユーザが正しい署名情報を埋め込まなかった場合、検証処理によって再現画像からそれが検出されるので、ユーザは不正をすることができない。また、サーバは、ユーザ側での 2 次暗号化の影響を受けた署名情報を埋め込み処理において知ることはできないので、サーバも不正をすることができない。さらに、検証局は、不正画像が発見されるまでは必要なく、不正画像発見以前に不正を行うことはできない。

【0057】なお、上記の検証処理の手順が公知で、ユーザとサーバとが互いにその結果を見届けあうならば、検証局はなくても各場合に依拠してユーザとサーバの不正は特定することができる。

【0058】〔第 2 の実施形態〕近年、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名称が記されないの、匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになる。このため、上述した電子透かしによる著作権者の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【0059】そこで、この第 2 の実施形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、

例えば、図 2 に示すようなシステム 200 により実現される。このシステム 200 は、上述した第 1 の実施形態におけるシステム 100 と同様の構成としているが、ユーザ端末装置 20 には、認証局 40 からの匿名公開鍵証明書が与えられる構成としている。

【0060】通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局と呼ばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSign や CyberTrust という企業がよく知られている。

【0061】よって、上述した第 1 の実施形態で述べた埋め込み処理中の 2) の手順においてサーバがユーザの契約情報を署名から確認する場合、図 2 の認証局 40 の証明書付きの公開鍵で確認することが考えられる。しかしながら、この証明書には通常、公開鍵の所有者の名称が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【0062】これに対して、公開鍵とその所有者との対応を認証局 40 が秘密に保持すれば、公開鍵の証明書に所有者の名称を記さないこともできる。このような匿名性を有する公開鍵の証明書を、以後「匿名公開鍵証明書」と呼び、そのような証明書付きの公開鍵を「証明書付き匿名公開鍵」と呼ぶ。そこで、ユーザ端末装置 20 は、上述した埋め込み処理中の 1) の手順において、契約情報と一緒に契約情報の署名、および署名情報 S を検査するための証明書付き匿名公開鍵を送れば、ユーザはデジタルデータの購入時に自分を匿名にすることができる。

【0063】よって、サーバ端末装置 10 には、利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局 40 に示してその公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定することができる。以上のことから、上述した第 1 の実施形態で述べた埋め込み処理中の 1)、2) の手順と、検証処理中の 1)、2) の手順とを以下のように変えることにより、ユーザのデジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【0064】以下、上記図 2 のシステム 200 における埋め込み処理、および検証処理について具体的に説明する。なお、上記図 2 のシステム 200 において、上記図

1 のシステム 1 0 0 と同様に動作する箇所には同じ符号を付し、その詳細な説明は省略し、異なる部分についてのみ具体的に説明するものとする。また、埋め込み処理の 1)、2) と検証処理の 1)、2) 以外については、上述した第 1 の実施の形態と同様であるため、その詳細な説明は省略する。

【0 0 6 5】[埋め込み処理]

1) まず、ユーザ端末装置 2 0 において、契約生成処理部 2 1 は、認証局 4 0 で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けてサーバ端末装置 1 0 に送る。

【0 0 6 6】2) 次に、サーバ端末装置 1 0 において、契約確認処理部 1 1 は、ユーザの公開鍵を認証局 4 0 の公開鍵によって検査するとともに、契約情報の署名をユーザの匿名公開鍵から確認し、その確認後に、少なくとも契約情報および証明書付き匿名公開鍵の一方から利用者情報 U を作成する。そして、第 1 の電子透かし埋め込み処理部 1 2 により上記契約確認処理部 1 1 で作成された利用者情報 U を要求された画像データ G に埋め込んだ後、1 次暗号化処理部 1 3 により 1 次暗号化処理 E 1 () を行い、得られたデータをユーザ端末装置 2 0 に送る。よって、ユーザ端末装置 2 0 には、1 次暗号化画像データ E 1 (G + U) の情報が送られる。以降、上述した第 1 の実施形態における埋め込み処理の 3) ~ 5) と同様の処理を行う。

【0 0 6 7】[検証処理]

1) サーバ端末装置 1 0 は、発見した不正画像 G w' から利用者情報 U' を抽出し、その抽出した利用者情報 U' と契約情報から分かる匿名公開鍵とを認証局 4 0 に示し、その匿名公開鍵に対応するユーザ名を聞く。

2) サーバ端末装置 1 0 は、不正画像 G W' と抽出した利用者情報 U'、およびユーザ名を検証局 3 0 に示し、ユーザへの検査を要求する。

そして、上述した第 1 の実施形態における検証処理の 3) ~ 7) と同様の処理を行う。

【0 0 6 8】以上述べたように、第 2 の実施形態によれば、ユーザはデジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【0 0 6 9】上述の第 1 および第 2 の実施形態に示した画像データ、および透かし情報の埋め込み処理によって得られるハッシュ値を含む種々のデータは、以下のような画像フォーマットで格納することができる。例えば、下記のような一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユーザが保存しておく必要があるハッシュ値およびその署名や、2 次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【0 0 7 0】一方、下記に示す FlashPix™ ファイルフォーマットでは、上記のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名などは、属性情報としてプロパティセットの中に格納しておくこともできる。

【0 0 7 1】まず、一般的な画像フォーマットについて説明する。一般的な画像フォーマットでは、図 3 に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。

【0 0 7 2】一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取るときに必要な情報や、画像の内容を説明する付帯的な情報が格納される。図 3 の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットのサイズなどの情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft 社の BMP フォーマットや CompuServe 社の GIF フォーマットなどが広く普及している。

【0 0 7 3】次に、FlashPix™ ファイルフォーマットについて具体的に説明する。以後説明する FlashPix™ (FlashPix は米国 Eastman Kodak 社の登録商標) ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図 4 および図 5 に示す。ファイル内の各プロパティやデータには、MS-DOS のディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図 4、図 5 において、影付き部分がストレージで、影なし部分がストリームである。画像データや画像属性情報はストリーム部分に格納される。

【0 0 7 4】図 4 において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像を Subimage と呼び、Resolution 0, 1, ..., n で示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報が Subimage Header に、また画像データが Subimage data に格納される。プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set, Image info. Property Set, Image Content Property Set, Extension list property Set がある。

【0 0 7 5】[各プロパティセットの説明] Summary info. Property Set は、FlashPix 特有のものではなく、Microsoft 社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj. St

reamには記憶部 (Strage) に関する一般的な情報が格納される。

【0076】Image Content Property Setは、画像データの格納方法を記述する属性である (図6参照)。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはJ P E G圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extension list property Set は、上記FlashPixの基本仕様に含まれない情報を追加する際に使用する領域である。さらに、ICC Profile の部分には、I C C (International Color Consortium) において規定される色空間変換のための変換プロファイルが記述される。

【0077】また、Image info. Property Setは、画像データを使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの下記のような情報を格納する。

- ・デジタルデータの取り込み方法／あるいは生成方法に関する情報
- ・著作権に関する情報
- ・画像の内容 (画像中の人物、場所など) に関する情報
- ・撮影に使われたカメラに関する情報
- ・撮影時のカメラのセッティング (露出、シャッタースピード、焦点距離、フラッシュ使用の有無など) の情報
- ・デジタルカメラ特有の解像度やモザイクフィルタに関する情報
- ・フィルムのメーカー名、製品名、種類 (ネガ／ポジ、カラー／白黒) 等の情報
- ・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
- ・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【0078】図5のFlashPix Image View Objectは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図5において、Global info. Property Set の部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報などが記述される。

【0079】また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの实体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、Result FlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【0080】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ID、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【0081】次に、画像データの取り扱いについて説明する。ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。図7に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図7において、最大解像度の画像は列×行が $X0 \times Y0$ で構成されており、その次に解像度の大きい画像は $X0/2 \times Y0/2$ であり、それ以降順次、列・行ともに $1/2$ ずつ縮小し、列・行ともに64画素以下あるいは互いに等しくなるまで縮小されていく。

【0082】このように画像データを階層化した結果、画像の属性情報として「1つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像フォーマットの項で説明したヘッダ情報と画像データとが必要となる (図3参照)。1つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記ImageContent Property Set中に記述される (図6参照)。

【0083】さらに、各解像度のレイヤの画像は、図8に示すように64画素×64画素でなるタイル毎に分割されている。画像の左上部から順次64画素×64画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、64画素×64画素を構築する。

【0084】FlashPix™では、それぞれのタイル中の画像データをJ P E G圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。J P E G圧縮は、ISO/IEC JT C1/SC29により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記1つのタイルがすべて同じ色で構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を1色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【0085】このようにタイル分割された画像データは、例えば図4のSubimage data ストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Header に格納されている (図9参照)。

【0086】【その他の実施形態】以上に述べた第1および第2の実施形態において、透かし情報の埋め込み

は、種々の手法によって実現できるが、例えば、「清水、沼尾、森本（日本IBM）：“ピクセルブロックによる静止画像データハイディング”，情報処理学会第53回全国大会，IN-11，平成8年9月」の文献や、「J. Cox, J. Kilian, T. Leighton and T. Shamoon (NEC)：“Secure Spread Spectrum Watermarking for Multimedia,” NEC Research Institute Technical Report 95-10.」の文献に示されるような公知の埋め込み手法によって実現できる。

【0087】また、1次暗号、2次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。また、全ての送信データにハッシュ値とその署名を付けて送ることもできる。さらに、1次暗号と2次暗号は、透かし情報の埋め込み処理においてサーバ側とユーザ側とで互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にDES (Data Encryption Standard) 等の暗号やハッシュ関数等を用いても良い。

【0088】また、上述の第1および第2の実施形態において、不正配布の検出はサーバ側が行っているが、1次暗号または2次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見をサーバ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者はサーバに限定されない。

【0089】また、サーバ端末装置10は、利用者情報Uだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、サーバ端末装置10で秘密の情報を埋め込みたい場合は、1次暗号化の後に埋め込み処理を行えば、署名情報と同様に1次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Uは、必ず1次暗号化の前にある必要はなく、1次暗号化の後に埋め込んでもよい（この場合、利用者情報Uの検出は、サーバまたは1次暗号の秘密鍵を知る者のみが行える）。

【0090】また、ユーザが複数のユーザ間で共通のプリンタや端末等を用いるユーザである場合、ユーザの署名情報および2次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。また、サーバ端末装置10からの1次暗号化情報は、ユーザ端末装置20からの契約情報による依頼がなくても、ネットワークやCD-ROM等によって広く配布されていても良い。

【0091】また、ユーザの署名情報Sは、公開鍵暗号方式によって生成されなくても、ユーザが契約情報等で定めた情報（暗証番号のような情報）等でも良い。また、米国では40ビット以上の暗号を用いる場合、暗号の悪用を防ぐために暗号鍵を管理する鍵管理局を必要と

する。そこで、検証局30に鍵管理局を兼ねさせることも可能である。よって、検証局30が2次暗号の鍵をあらかじめ管理している場合には、不正画像の監視も検証局30が行えば、検証処理1)～3)は検証局30が単独で行うことができる。サーバ端末装置10での1次暗号の鍵は、同じ検証局30によって管理されていてもよいし、他の鍵管理局によって管理されていてもよい。また、サーバ端末装置10やユーザ端末装置20の鍵は、鍵管理局が生成し、配布してもよい。

10 【0092】

【発明の効果】上述の説明から明らかなように、本発明の電子透かし方式および電子情報配布システムによれば、デジタルデータを不正にコピーして配布を行った際にその不正行為および不正行為者を確実に認識することができ、これによって不正を確実に防止することが可能となり、デジタルデータの不正配布に関して安全なシステムを実現することができる。また、上記電子透かし方式を用いて電子透かしを埋め込んだ画像データをファイルできる画像ファイル装置で、特に埋め込まれた電子透かし情報を比較的容易に確認することのできる画像ファイル装置を得ることができる。さらに、このシステムによってユーザの匿名性や暗号の悪用を防ぐ鍵管理局への応用も容易に実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示した電子透かしシステムを説明するための図である。

【図2】本発明の第2の実施形態を示した電子透かしシステムを説明するための図である。

【図3】一般的な画像フォーマットを示す図である。

30 【図4】FlashPixTMファイルフォーマットの例を示す図である。

【図5】FlashPixTMファイルフォーマットの例を示す図である。

【図6】FlashPixTMファイルフォーマットのImage Content Property Setに格納される属性情報を示す図である。

【図7】それぞれ解像度の異なる複数の画像から構成される画像ファイルの例を示す図である。

40 【図8】各解像度のレイヤの画像のタイル分割の様子を示す図である。

【図9】タイル分割された画像データに関する属性情報を示す図である。

【図10】従来の電子透かしシステムを説明するための図である。

【図11】図10に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【図12】図11に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【符号の説明】

50 10 サーバ端末装置

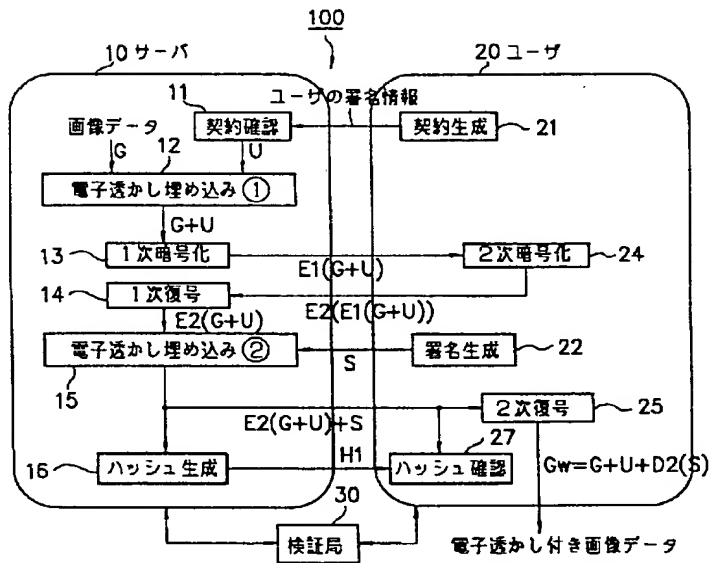
21

22

- 11 契約確認処理部
- 12 第1の電子透かし埋め込み処理部
- 13 1次暗号化処理部
- 14 1次復号処理部
- 15 第2の電子透かし埋め込み処理部
- 16 ハッシュ生成処理部
- 20 ユーザ端末装置
- 21 契約生成処理部

- 22 署名生成処理部
- 24 2次暗号化処理部
- 25 2次復号処理部
- 27 ハッシュ確認処理部
- 30 検証局端末装置
- 40 認証局端末装置
- 100 電子情報配布システム
- 200 電子情報配布システム

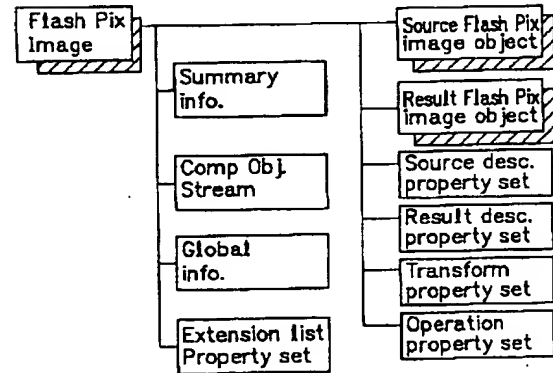
【図1】



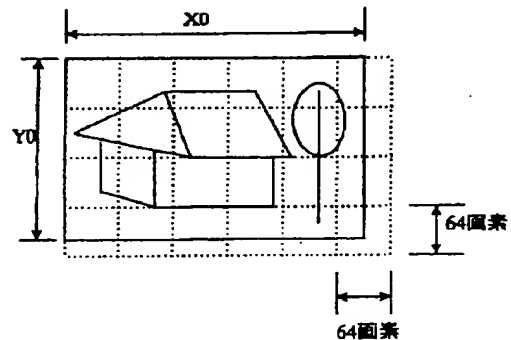
【図3】

画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数(幅)
	Y方向ピクセル数(高さ)
	深さ方向サイズ
	圧縮の有無
	解像度
	ビットマップへのオフセット
	カラーパレットサイズ
画像データ部	ビットマップ

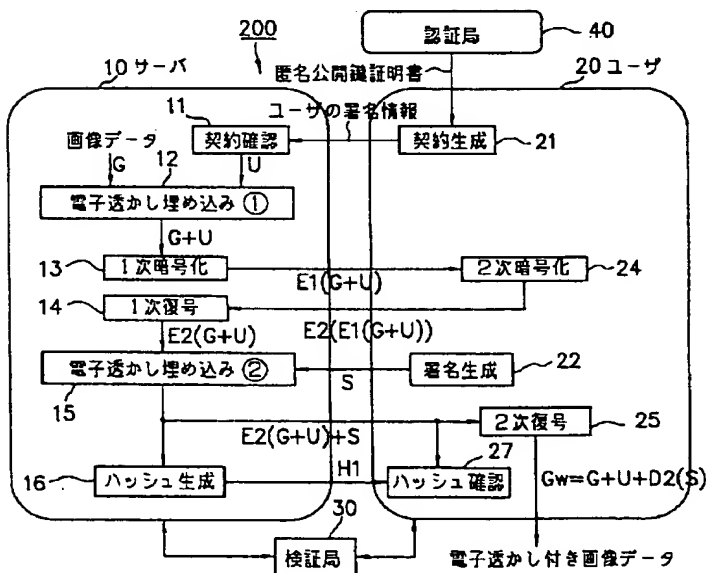
【図5】



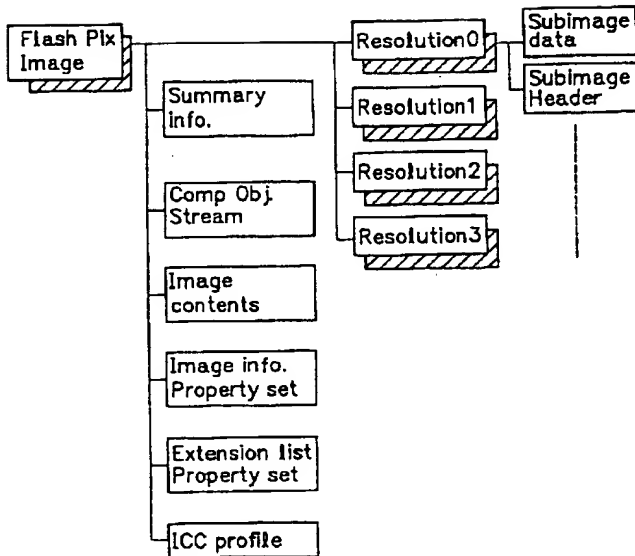
【図8】



【図2】



【図 4】



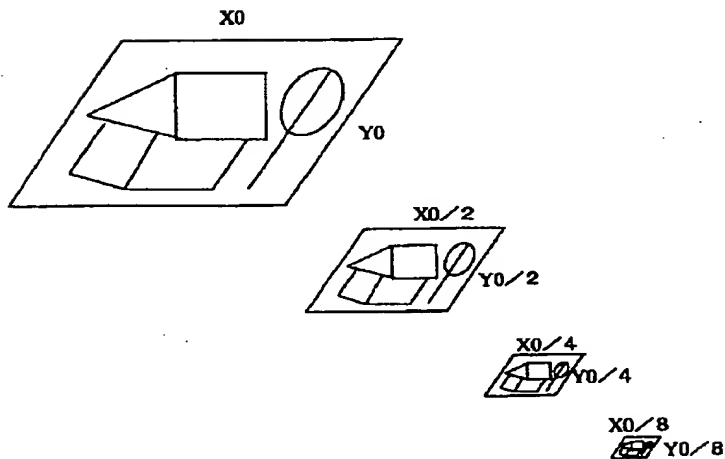
【図 6】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4 VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

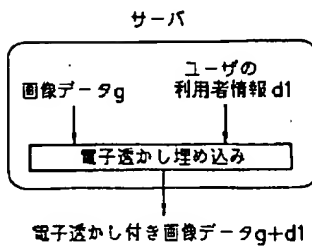
【図 7】



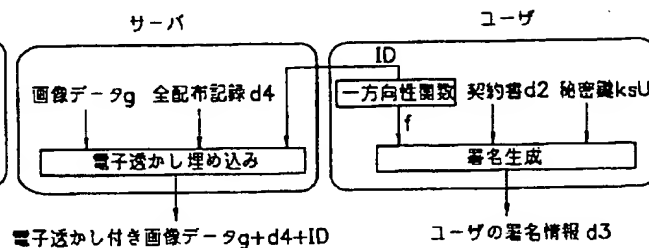
【図 9】

フィールド名	長さ	バイト
画像の幅	4	4-7
画像の高さ	4	8-11
タイルの総数	4	12-15
タイルの幅	4	16-19
タイルの高さ	4	20-23

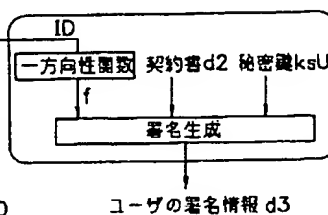
【図 10】



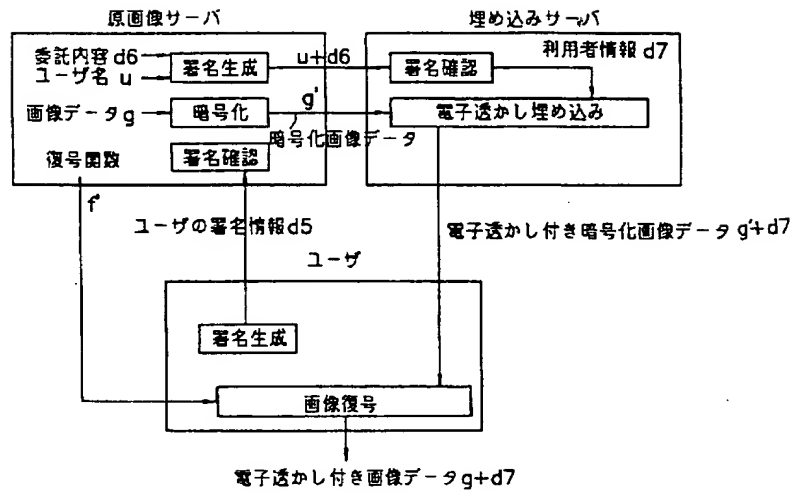
【図 11】



ユーザ



【図 1 2】



フロントページの続き

(51) Int. Cl. ⁶

H 0 4 L 9/32
H 0 4 N 7/08
7/081

識別記号

F I

H 0 4 L 9/00
H 0 4 N 7/08

6 7 5 D
Z

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.